VULNERABILITY ASSESSMENTS VS PENETRATION TESTING: WHAT'S THE DIFFERENCE?

Vulnerability assessments and penetration testing are techniques used by IT security teams to identify and resolve security issues in an organization's IT networks, infrastructure, applications, and other areas. These assessments and tests share a common goal, but the methods and tools used to find and fix security flaws are different. Both are essential to a clear and complete understanding of risks across the IT ecosystem and should be used together to identify and remediate potential attack vectors and technological weaknesses.

Vulnerability Scanning and Assessment Principles

A vulnerability scanning and assessment tool:

- Uses a broad approach to identify flaws and vulnerabilities across the enterprise
- Scans against a list of known risks, provided through a vulnerability database
- Can run automatically and on a scheduled basis
- Is made up of four main areas: User interface, vulnerability list, scan engine, and reporting tool
- Can prioritize vulnerabilities based on severity, urgency, and ease of fix
- Will provide suggestions for fixing identified flaws

Vulnerability scanning and assessment allows for early and reliable identification of IT weaknesses. These tools depend on the software vendor regularly identifying threats and integrating them into

the vulnerability database. Because these tools assess previously known security issues, they will also highlight restorative actions to patch those flaws. Vulnerability assessment focuses on reliable identification of risks and remediation of IT flaws across the enterprise.

Penetration Testing Principles

Penetration testing:

- Uses a targeted approach to attempt to break through IT security and defenses
- Tries to simulate a real-life attack by hackers and other bad actors
- Attempts to gain access to critical systems and sensitive information
- Adapts according to resistance and tries to find new attack vectors
- Is not as concerned with previously-identified, specific vulnerabilities
- Can use a variety of software, hacks, scripts, and other methods to penetrate defenses

Penetration testing allows for a deep understanding of how the IT ecosystem could be breached. It uses a combination of specialist tools, an understanding of a hacker's approach, and other techniques like social engineering to achieve results. Penetration testing focuses on how a bad actor could actually breach IT systems through a targeted attack.

Vulnerability Assessments and Penetration Testing Across Different Environments

With the migration of infrastructure, applications, and data into the cloud, both vulnerability assessments and penetration testing must work across all IT environments. Whether you operate onsite IT, or rely on a private, public, or hybrid cloud, make sure you use tools that can identify vulnerabilities wherever they may be, and can also deal with the integrations and connections between these environments.

Main Differences Between Vulnerability Assessment and Penetration Testing

Now that we've explained the principles of both approaches, let's explore the main differences:

- Vulnerability assessments are list-based; penetration tests are goal-based.
- Penetration tests are adaptable based on that unique test; vulnerability assessments use a consistent, tool-based method.
- Vulnerability assessments look at a wide range of risks; penetration testing uses a much more targeted approach.

Organizations should use penetration testing and vulnerability assessments together, but if you need to prioritize, you can look at the maturity of your IT security operations.

Vulnerability Assessments, Penetration Testing, and IT Maturity

Less mature IT security will get more benefit from vulnerability assessments and scanning. Because these tools analyze the entire IT ecosystem, they will expose the most common attack vectors and security flaws. These tools offer comprehensive reports and mitigating actions. This can make

resource allocation and restoration quicker and easier.

Vulnerability scanning is an ideal tool when an organization knows it has security issues, but not where they are. Since it uses previously-identified vulnerabilities, it can quickly and thoroughly test all your systems against those vulnerabilities.

If your organization already has mature IT security, vulnerability assessment can still be useful. Even well-established software can have bugs, and scheduling security scans means you can patch those flaws as they're reported. New projects and implementations also benefit from vulnerability scanning, so you can test and fix flaws in the development or staging environment before moving into production.

Penetration testing is most useful for organizations with a strong maturity in their IT security operations. Because penetration testing is tailored to your unique infrastructure, applications, and defenses, it can give you early insight of how a hacker would compromise your systems. Penetration testing is also ideal if you've identified or successfully repelled previous hackers, so you can fix flaws that would allow them to further penetrate your systems.

TrueSight Vulnerability Management

TrueSight Vulnerability Management will identify flaws and security risks across all IT environments. It provides automated security testing and remediation, container security, built-in resolutions, out-of-the-box security configurations and policies, and extensive integration across your IT environment.

You can take advantage of powerful dashboards and reporting, streamlined workflows, blind spot awareness, service management support, process improvement, and comprehensive import and export.

Learn how TrueSight Vulnerability Management can help reduce your organization's IT risk.